Statement
Of
Robert S. Mueller, III
Director of the Federal Bureau of Investigation
Before The
United States House of Representatives
Committee on Appropriations
Subcommittee on Science, State, Justice and Commerce
September 14, 2005

Good morning, Mr. Chairman, Representative Mollohan, and Members of the Subcommittee. I am pleased to appear before you today to update you on the ongoing transformation of the FBI. I would first like to express my gratitude for the continued support and guidance you have provided the FBI as we continue our efforts to ensure that we are able to address current threats and keep America safe from those who would do us harm.

Probably at no time in history has the FBI changed on such a large scale as in the past four years. Today, I want to discuss these changes in light of evolving threats and improvements in our ability to respond to those threats, both old and new.

The FBI has always changed to meet evolving threats -- from the "gangster era" through the Cold War. It was because crime had begun to cross state lines that the Bureau of Investigation was first established in 1908, under then President Theodore Roosevelt.

Nearly 100 years later, criminal activity not only crosses state lines, it traverses international boundaries with the stroke of a computer key. Crime is more diverse than ever before. It includes terrorism, violent gangs, illegal weapons trade, and the trafficking of human beings.

Mr. Chairman, our ability to confront and defeat these threats depends on our ability to develop and utilize three critical capabilities: intelligence, technology and partnerships.

INTELLIGENCE

For our purposes, intelligence means vital information about those who would do us harm. The FBI has always used intelligence in criminal and national security investigations. It is how we fought Nazi spies during World War II, Soviet espionage during the Cold War, and La Cosa Nostra in the eighties and nineties.

FBI National Security Branch

On June 28, 2005, the President issued a memorandum acknowledging the substantial efforts the United States Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI) have made in strengthening their national security capabilities and coordinating effectively with other elements of the Government. The President also determined that additional action is required to meet evolving challenges to the security of the United States. The President therefore directed the Attorney General to implement the recommendation of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (WMD Commission) that the FBI establish a "National Security Service." The President instructed the Attorney General to combine the missions, capabilities, and resources of the counterterrorism, counterintelligence, and intelligence elements of the FBI under the leadership of a senior FBI official.

In implementing this directive, the FBI is committed to fulfilling our statutory responsibilities for the conduct of national security operations and the protection of civil liberties. We are responsible for ensuring the timely execution of programs, policies and directives established or developed by the Director of National Intelligence (DNI). In keeping with the high level of public trust required to operate a combined intelligence and law enforcement agency, the FBI will carry out its mission with full respect for the constitutional and civil rights of the American people.

The FBI's provisional plan, which reflects the guidance of the Attorney General and is under consideration by the DNI, outlines steps the FBI would take to implement the President's directive. The ultimate goal is to build upon the strength of the FBI's existing counterterrorism, counterintelligence, and intelligence capabilities by creating an integrated service that will better contribute to the national intelligence effort in executing the FBI's national security missions. The plan will effectively expand efforts the FBI has undertaken since September 11, 2001, and leverage the FBI's existing law enforcement capabilities. We are working with the DNI in completing a Report to the President further defining the NSB.

The plan will be implemented through the National Security Branch (NSB), which will integrate the FBI's primary national security programs under the leadership of an Executive Assistant Director for the National Security Branch (EAD-NSB), and through policies and initiatives designed to enhance the capability of the entire Bureau to support its national security missions. Last month, we announced that Gary Bald has been selected to serve as the first EAD-NSB. Mr. Bald brings to this position a wide range of operational and leadership experience,

which he has demonstrated in his nearly 28 years of service with the FBI. As the EAD for Counterterrorism and Counterintelligence, Mr. Bald has had overall responsibility for all aspects of the FBI's two highest priority investigative programs, which, in addition to terrorism and counterintelligence, include espionage, counter-proliferation and foreign intelligence matters. Mr. Bald's deputy will be Philip Mudd, a highly accomplished 20-year veteran of the Intelligence Community, who currently serves as the Deputy Director of the CIA's Counterterrorism Center. Mr. Mudd brings to this position his extensive expertise in intelligence operations and analysis, as well as an in-depth knowledge of international terrorism and the Middle East.

The NSB will consist of the Counterterrorism Division (CTD), the Counterintelligence Division (CD), and the Directorate of Intelligence (DI). The EAD-NSB will report to the Deputy Director and will exercise my authorities over the activities of the NSB's components.

The EAD-NSB will replace the existing positions of Executive Assistant Director for Intelligence and Executive Assistant Director for Counterterrorism/Counterintelligence and will have the combined authority of these two positions.

The EAD-NSB will serve as the FBI's lead intelligence official and will communicate with the DNI to ensure responsiveness to DNI guidance, and to facilitate coordination with other elements of the Intelligence Community.

The NSB will be responsible for the continued development of a specialized national security workforce through programs designed to recruit, train, develop, and retain professionals who have the skills necessary to the success of the FBI's national security missions. This workforce will be developed in consultation with the DNI to ensure consistency with established Intelligence Community workforce standards.

The NSB will have full access to information from all counterterrorism, counterintelligence, and intelligence operations, as well as information about all of the Bureau's sources of information. The NSB will manage and direct field activities and hold personnel accountable through evaluations of individual performance, the regular inspection process, and program-specific reviews.

Consistent with the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), the FBI's Directorate of Intelligence (DI) will continue to provide clear guidance to agents and analysts to ensure that all investigative products are reviewed by the DI for their intelligence value, and that national intelligence priorities promulgated by the DNI and endorsed by the National Security Council (NSC) and Homeland Security Council (HSC) drive collection and information sharing in every FBI division.

The NSB will enforce the implementation of standardized intelligence processes across component divisions, consistent with DNI guidance. The NSB also will ensure that critical enabling processes, such as training, hiring, career development, information technology support, and secure facilities construction, support intelligence priorities and conform to DOJ

and FBI policies and DNI standards.

The creation of a unified management structure to oversee the FBI's national security components will ensure that NSB activities will be coordinated with other Intelligence Community agencies under the DNI's leadership.

To achieve this level of coordination, the NSB will work with the FBI's Chief Information Officer (CIO), the Office of the DNI Chief Information Officer (ODNI/CIO), and the Associate Director of National Intelligence for Science and Technology to ensure that appropriate networks and systems are developed consistent with DNI standards. The NSB also will expand its Sensitive Compartmented Information Facilities (SCIF) and access to the Intelligence Community's Intelink Top Secret information sharing environment.

To further improve coordination with the DNI, I have designated the EAD-NSB the lead FBI official responsible for coordination with the DNI and the rest of the Intelligence Community. The EAD-NSB will ensure appropriate FBI representation in the interagency process and participation in Intelligence Community activities as required by the DNI.

In consultation with the DNI and the Attorney General, EAD Bald and I will regularly examine the national intelligence priorities, promulgated by the DNI and endorsed by the NSC and HSC, to determine whether NSB resources are being appropriately allocated to meet U.S. national security and law enforcement needs. The FBI, DOJ and the Office of the DNI will also establish a process to ensure that the DNI has appropriate insight into the performance of the NSB.

FBI Intelligence Workforce

In support of the President's directive, the FBI will continue to establish programs and practices for building a national security workforce. The FBI's national security workforce is broadly defined to consist of all personnel at FBI headquarters and in the field who perform the national security missions of the FBI, including the full complement of personnel within the CTD, CD, and DI, and personnel outside the NSB who perform intelligence and national security-related work in support of the NSB. The FBI will develop this workforce through programs designed to recruit, train, develop, and retain professionals who have the skills necessary for the success of its national security missions.

The FBI is implementing several workforce programs to build its national security capabilities, including the Special Agent Career Path and the Intelligence Career Service. These programs are designed to enhance and specialize the national security workforce and to create training and development opportunities for agents, analysts, linguists, and physical surveillance specialists in the FBI's national security programs.

Throughout the development of the FBI's national security workforce, the NSB will work with the DNI, including the Assistant Deputy DNI for Training and Education and the Chief

Human Resource Officer, to ensure adherence to DNI standards.

Recruitment

The NSB will continually refine its recruiting standards, consistent with Intelligence Community standards, to ensure that the workforce has the necessary substantive expertise to meet national security needs. The NSB will ensure that the workforce has educational and/or professional experience in relevant regional, cultural, scientific, economic, and technical areas as well as operational, analytic, linguistic, and scientific capabilities.

Special Agent Career Development

The FBI's recruitment, hiring, training, and assignment of Special Agents will promote specialization and development of counterterrorism, counterintelligence, and intelligence expertise while providing a solid foundation in law enforcement and constitutional protections. All Special Agents will be trained in both intelligence and law enforcement functions. They will also receive extensive training on upholding the Constitution and protecting civil liberties. As the WMD Commission recognized, agents should be able to move between the use of intelligence and law enforcement tools and to conduct all activities consistent with the Attorney General Guidelines and constitutional protections.

Training

All Special Agents will continue to participate in the FBI's basic training course of instruction at the FBI Academy in Quantico, Virginia. The intelligence training component offered in this basic course to all new agents will be enhanced under the guidance of the EAD-NSB consistent with DNI standards.

Advanced training for agents in national security career paths will cover management, targeting, asset validation, source development, and recruitment. While the FBI develops this training in conjunction with the DNI, it is expected that new NSB personnel will attend courses at the Intelligence Community's other educational centers. The FBI will work with the DNI to ensure that an appropriate provisional arrangement is made in this regard while a more permanent program, including the allocation of sufficient resources, is established.

In addition to advanced training, agents will participate in other developmental opportunities throughout their careers. Joint assignments to other Intelligence Community agencies will be made an integral (and in many cases, required) component of the national security career paths. Recognizing the importance of centralized management to the FBI's national security programs, headquarters assignments in NSB components also will be part of the career development process.

Career Paths

The career path currently under development for Special Agents contemplates four milestones. As with all agents, they will complete the new agent curriculum at the FBI Academy, Quantico, Virginia and thereby receive a strong grounding in law enforcement training. From there, they will build on the broad foundation of basic training and will participate in developmental opportunities designed to build program-specific expertise. Afterwards, agents will be assigned to a counterterrorism or counterintelligence squad or Field Intelligence Group (FIG) in one of the larger field offices. And finally, agents will further develop specialization and expertise in national security programs and progress as recognized leaders in either investigative or management positions.

Intelligence Career Service

Consistent with the IRTPA, the FBI has developed an Intelligence Career Service (ICS) that provides career paths for Intelligence Analysts, Language Analysts, and Physical Surveillance Specialists. ICS programs and policies are, and will remain, consistent with Intelligence Community standards articulated by the DNI.

These career paths were established based on competency models for each ICS career specialty. All members of the ICS receive a minimum of five weeks of joint training focused on the core competencies required of the entire ICS. This is followed immediately by specialized training for intelligence analysts, language analysts, special surveillance personnel, and lookouts. This initial training will be supplemented by advanced and specialized training throughout individuals' careers and by developmental opportunities, including details to other Intelligence Community agencies.

The new career paths allow members of the ICS to reach the executive level through both technical and management tracks. Pursuant to the IRTPA, to the maximum extent practicable, I will ensure that the successful discharge of advanced training courses, and of one or more assignments to another element of the intelligence community, is a precondition to advancement to higher level intelligence assignments within the Bureau.

TECHNOLOGY

The second critical capability -- technology -- helps us collect, analyze, and share intelligence. We recognize the need for a fully operational modern information technology infrastructure, one that enables effective information sharing that will close the communication gap with our law enforcement partners and the intelligence community. Our overriding goal is to provide the right information, to the right people, at the right time.

The FBI's commitment to delivering enhanced technology capabilities remains resolute. Our efforts with regard to the Trilogy project resulted in increased understanding of program management and technical expertise. The lessons learned have better positioned us to shape the FBI's next-generation electronic information management system. Successful deployment of SENTINEL remains a top priority.

SENTINEL is the first step in our deployment of a Service Oriented Architecture (SOA) which will serve as a platform for gradual deployment of capabilities and services needed by all FBI divisions. We will gradually roll-out key technical services, such as automated workflow, search capabilities, records and case management, and reporting protocols, through the SENTINEL program. The SOA approach will raise our business practices to the next level by providing enhanced capabilities, new services, and better efficiency, while also ensuring a smooth transition from our legacy applications to a more state-of-the-art technical platform. The SOA will enhance efficiency and effectiveness of many FBI programs and further support our mission by helping manage our investigative, administrative, and intelligence needs, while also improving ways to encourage information sharing among our counterparts.

As you are aware, we are proceeding with the acquisition of the capabilities to be provided by the SENTINEL program. After extensive industry and internal reviews, the Request for Proposal was approved and released on August 5th. We are currently awaiting proposal responses from industry, and expect to award the contract in the next several months, pending the completion of the reprogramming notification to Congress. SENTINEL will be deployed in four phases using program management tools and best industry practices to measure each stage of development for the SENTINEL system and to minimize risk. The phased roll-out will also facilitate ease of deployment, user transition, and training.

We will continue to work with this subcommittee and other Congressional committees, the Administration, DOJ, DNI, DHS, GAO, NAPA, CRS and the FBI Advisory Board to coordinate the next steps in implementing the SENTINEL program.

PARTNERSHIPS

In addition to intelligence and technology, the third critical element to improving our capabilities is partnerships. Partnerships at all levels -- local, state, federal, and international -- help us share what we know.

At the state and local level, our Joint Terrorism Task Forces (JTTF) are the eyes and ears of communities around the country. Working side-by-side, members from intelligence and law enforcement agencies track down each and every counterterrorism lead, no matter how insignificant it may seem. In the last four years, we have increased the JTTFs from 35 to 103.

In addition to the JTTFs, our Regional Computer Forensics Labs combine partnerships and technology. These state-of-the-art regional facilities are highly specialized laboratories that provide forensic examinations of digital evidence. Six labs are up and running, and eight more are in the works. In each one, law enforcement agencies from all levels of government train, work, and share information together. In particular, they make use of new forensics capabilities to address terrorism, cyber crime, and identity theft, as well as other crimes.

Not only are we cooperating better at the state and local level, we are also working more

closely with our partners at the national level. At the National Counterterrorism Center -- formerly Terrorist Threat Integration Center (TTIC) -- federal agencies work side-by-side analyzing terrorist threat information. The Center receives foreign intelligence information lawfully collected by its members. This includes international terrorism information collected by the law enforcement community.

Cooperation has improved globally as well. FBI Agents are working with our law enforcement partners from Rome to Romania. We are gathering intelligence in Iraq and Afghanistan. These international partnerships are critical if we hope to be successful in the future.

Department of Defense

I am proud of our efforts and partnership with the Department of Defense (DoD). In an effort to support the Global War on Terrorism and the information sharing initiatives, the FBI's Criminal Justice Information Services (CJIS) Division, in conjunction with the DoD's Biometric Fusion Center (BFC), has been working to share data collected by military troops deployed internationally. This data consists of fingerprints, photographs and biographical data of military detainees, or individuals of interest as national security threats to the United States.

In order to ensure quality and interoperability of all fingerprint data collected in support of the Global War on Terror, a DoD memorandum was issued in February 2004 directing that all new DoD acquisitions of fingerprint data collected must conform with the Electronic Fingerprint Transmission Specification (EFTS) derived from the American National Standards Institute/National Institute of Standards and Technology. The memorandum also advised that the data must be collected by certified equipment that is interoperable with the FBI's IAFIS.

The FBI's CJIS Division and the DoD cooperatively developed the Automated Biometric Identification System (ABIS). The DoD ABIS consolidates, formats, and exchanges data equivalent and consistent to the FBI’s current State/County/Local law enforcement model. The ABIS provides the DoD the ability to gather, store, share, and enter the information into the FBI’s IAFIS, which allows the FBI to disseminate appropriate information to other government and law enforcement agencies.

The DoD appointed its Biometric Fusion Center as the channeling agency to receive data collected from various military service branches and then forward it to the FBI via the CJIS Wide Area Network. The ABIS contains biometric information, fingerprint images, and their related features and may also contain additional identification data such as deoxyribonucleic acid (DNA) or a photograph. Engineers linked the two systems so that DoD biometric information could be shared with local, state, and Federal law enforcement. Future tests will explore the advantages of IAFIS searching ABIS in order to share additional DoD information.

The FBI's growing biometric-based terrorism file is making substantial contributions to the homeland security effort by increasing the odds that potential terrorists will be intercepted by

United States Officials.

Counterterrorism Initiatives

Mr. Chairman, the following are just a few of the unclassified examples of successes in the war against terrorism that would not have been possible without extensive cooperation and coordination with our partners.

- Operation Crevice was a joint US, UK, Pakistani, and Canadian investigation of a group of individuals targeting unidentified Western targets. Through joint investigation by intelligence and law enforcement agencies in these countries, components for explosive devices were recovered and numerous individuals overseas were arrested. An investigation conducted by the FBI led to the arrest of an individual in the US who was charged with terrorism offenses.

- Operation Rhyme was a joint US-UK investigation into a UK-based terrorism subject and his associates. Investigation by the FBI and our British counterparts led to the identification of several individuals in the US who maintained contact with the main subjects of the investigation. The main subject and two of his associates have been indicted in the US for terrorism-related offenses.

- The FBI's Terrorism Financing Operations Section (TFOS), in concert with the Internal Revenue Service and the Central Intelligence Agency, are partners with the Saudi Mabahith in the Joint Terrorism Financing Task Force based in Riyadh, Saudi Arabia. This task force specializes in facilitating counterterrorism financing investigations with leads connected to the Kingdom of Saudi Arabia. In conjunction with its participation on this task force, TFOS has also aggressively pursed a rigorous, multi-phase training program for the Saudi Mabahith officers assigned to the task force.

Laboratory

The Terrorist Explosive Device Analytical Center (TEDAC) is an FBI led initiative and interagency supported program that is based in the FBI Laboratory, Quantico, Virginia. It is committed to establishing a single federal program responsible for the worldwide collection, complete analysis and timely dissemination of intelligence regarding terrorist IEDs. Prior to the TEDAC initiative, there were a number of organizations responsible for the technical analysis of Improvised Explosive Devices (IED). The aggressive use of IED technology by the insurgents in Iraq overwhelmed these limited resources. TEDAC fills a vital role as a clearing house and forensic evidence collector for IED material. Other organizations will continue to provide technical analysis and countermeasures development in coordination with TEDAC.

The TEDAC receives and exploits raw intelligence and information, component hardware and other physical items from various members of the Explosive Ordnance Disposal (EOD) and

IED community worldwide. Functioning as the repository for all information and items received, the TEDAC conducts a full range of forensic analysis deemed appropriate on each item. TEDAC reports the results of these forensic analyses to the IED community and maintains a database for all information developed. TEDAC provides link analysis of all intelligence developed and provides devices to members of the IED community for any further exploitation deemed necessary to facilitate research, development and engineering imperatives. TEDAC is committed to providing international, federal, state and local law enforcement and bomb squads with current information relating to terrorist IEDs being used overseas. To date, the TEDAC has received over 3,000 devices for analysis with the majority of those devices coming from the Iraq Theater of Operations. In addition, it has made over 350 forensic and technical associations between devices.

Since its inception, TEDAC has received support from a wide variety of U.S. explosives and intelligence entities in the analysis of IEDs, including specialists from the Bureau of Alcohol, Tobacco, Firearms and Explosives, Federal Air Marshal Service, Technical Support Working Group, Navy Research Lab, National Ground Intelligence Center, Naval EOD Technical Division, Army Research, Development and Engineering Command, U.S. Marine Corps IED Working Group and numerous other federal government agencies, and components of the Department of Defense.

Today, cases with an international nexus have become the rule rather than the exception. President Wilson could have been talking about law enforcement today when he said, "Friendship is the only cement that will ever hold the world together."

In this era of globalization, working side-by-side is not just the best option, it is the only option.

Mr. Chairman, by building our intelligence capabilities, improving our technology, and working together, we can and we will continue to develop the capabilities we need to succeed against the threats of the future.

Thank you for your continued support and interest in the FBI.